Data Privacy and Cybersecurity in the Indian Hospitality Sector: Challenges, Legal Framework, and Strategic Solutions

Mr. Arpan Tah

PhD(Pursuing),MBA(TOURISM)(Gold Medalist),B.E.
Research Scholar in the Department of Tourism Management,The University of Burdwan.
Visiting Faculty of B.B.A Department at B.I.M.S College (Affiliated under The University Of Burdwan).
Former Head of the Department of B.B.A & B.B.A TOURISM & HOSPITALITY at AMEX College
(Affiliated under The University Of Burdwan)

Mr. Swarnadeep Goswami

MBA(HR),SAP(Sales & Distribution)
Assistant Professor in B.B.A Department at B.I.M.S College(Affiliated under The University Of Burdwan).
Former Assistant Professor at Swami Vivekananda Institute of Mordern Science
(Affiliated under M.A.K.A.U.T)

Dr.Tripti Das
PhD, M.T.T.M, Amadeus GDS Trained
Guest Faculty of B.B.A Tourism & HOSPITALITY at AMEX College
(Affiliated under The University Of Burdwan)

How to Cite this Article:

Goswami, S. & Tah, A. (2026). Data Privacy and Cybersecurity in the Indian Hospitality Sector: Challenges, Legal Framework, and Strategic Solutions. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.266

https://doi.org/ 10.55041/ijcope.v2i4.266

Abstract

The Indian hospitality sector, encompassing hotels, resorts, restaurants, and travel services, is increasingly reliant on digital technologies for operations, customer engagement, and service delivery. This digital transformation has significantly increased the volume and sensitivity of personal data collected, thereby raising concerns related to data privacy and cybersecurity. With the enactment of the Digital Personal Data Protection (DPDP) Act, 2023 and its operational Rules in 2025, India has entered a new era of data governance. This study examines the challenges, risks, legal frameworks, and cybersecurity practices within the Indian hospitality industry. Using qualitative research methods and secondary data analysis, the paper explores compliance gaps, emerging threats, and strategic measures required to safeguard customer data. The study concludes that robust cybersecurity infrastructure, regulatory compliance, employee training, and data governance frameworks are critical for ensuring trust and sustainability in the sector.

Keywords: Data Privacy, Cybersecurity, Hospitality Sector, India, DPDP Act 2023, Data Protection, Digital Security

Introduction

The Indian hospitality sector has undergone a profound transformation over the past decade, driven by rapid digitalization, globalization, and changing consumer expectations. Hotels, resorts, travel agencies, and food service providers increasingly rely on digital platforms such as online booking engines, mobile applications, customer relationship management (CRM) systems, and cloud-based property management systems (PMS). These technologies enable seamless guest experiences, personalized services, and operational efficiency. However, they also necessitate the large-scale collection, storage, and processing of personal data.

Hospitality organizations routinely collect sensitive information including identity documents, financial details, travel history, biometric data (in some cases), and behavioral preferences. This data is not only essential for service delivery but also valuable for targeted marketing and business analytics. Consequently, the sector has become a lucrative target for cybercriminals seeking to exploit vulnerabilities in data systems.

The increasing frequency of cyberattacks such as ransomware, phishing, and data breaches has raised serious concerns about data privacy and cybersecurity in the hospitality industry. Moreover, the introduction of India's Digital Personal Data Protection (DPDP) Act, 2023 has brought regulatory scrutiny and compliance obligations to the forefront. The Act mandates organizations to adopt transparent, accountable, and secure data handling practices.

In this context, the intersection of hospitality management and data protection law presents a critical area of study. Ensuring data privacy is no longer just a technical issue but a strategic, legal, and ethical responsibility for hospitality organizations.

Objectives of the Study

The primary objective of this study is to explore the growing importance of data privacy and cybersecurity within the Indian hospitality sector in light of technological advancements and regulatory developments.

Specifically, the study aims to analyze the various data privacy challenges faced by hospitality businesses, including issues related to excessive data collection, lack of transparency, and third-party data sharing. It also seeks to examine the cybersecurity threats that affect the sector, such as hacking, malware attacks, and system vulnerabilities.

Another key objective is to evaluate the legal and regulatory framework governing data protection in India, particularly the implications of the DPDP Act, 2023 and related rules. The study further intends to assess the level of preparedness and compliance among hospitality organizations and identify gaps between regulatory expectations and industry practices.

Finally, the research aims to provide practical recommendations and strategic solutions that can help hospitality businesses enhance their data protection mechanisms, ensure legal compliance, and build customer trust.

Research Methodology

This study adopts a qualitative and exploratory research design, which is suitable for analyzing emerging issues such as data privacy and cybersecurity in a sector-specific context. Given the evolving nature of digital threats and regulatory frameworks, the research relies primarily on secondary data sources.

The data for this study has been collected from a wide range of sources, including government publications, legal documents, industry reports, academic journals, cybersecurity white papers, and news articles. Key legislative documents such as the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000 have been critically analyzed to understand the legal landscape.

A thematic analysis approach has been used to identify recurring patterns and key issues related to data privacy and cybersecurity in the hospitality sector. The study also incorporates a comparative perspective by referencing global practices and standards in data protection.

This methodology allows for a comprehensive understanding of the subject while ensuring academic rigor and relevance.

Literature Review

The existing body of literature highlights the increasing vulnerability of the hospitality sector to data privacy breaches and cyber threats. Researchers have emphasized that the industry's dependence on digital technologies and its handling of large volumes of personal data make it particularly susceptible to cyber risks.

Studies on data privacy indicate that hospitality businesses often lack robust data governance frameworks, leading to issues such as unauthorized data access, inadequate consent mechanisms, and poor data retention practices. Scholars have also pointed out that many organizations collect more data than necessary, thereby increasing their exposure to regulatory and security risks.

In the area of cybersecurity, research has identified common threats such as phishing attacks, ransomware, malware infections, and insider threats. The integration of Internet of Things (IoT) devices in hotels, such as smart locks and connected appliances, has further expanded the attack surface.

Legal scholars have analyzed the impact of data protection laws on business practices, noting that regulations like the General Data Protection Regulation (GDPR) in Europe have significantly influenced global data protection standards. In India, the DPDP Act, 2023 is seen as a landmark legislation that aims to align the country with international best practices.

Overall, the literature underscores the need for a holistic approach that combines technological solutions, legal compliance, and organizational awareness to address data privacy and cybersecurity challenges.

Data Privacy Issues in the Indian Hospitality Sector

Data privacy concerns in the Indian hospitality sector arise primarily from the extensive collection and processing of personal data. One of the major issues is excessive data collection, where hotels gather more information than is necessary for service delivery. This includes sensitive details such as identification numbers, travel itineraries, and personal preferences.

Another significant issue is the lack of transparency in data handling practices. Many hospitality organizations do not clearly inform customers about how their data will be used, stored, or shared. Privacy policies are often complex and not easily understandable, leading to a lack of informed consent.

Third-party data sharing further complicates the situation. Hospitality businesses frequently collaborate with online travel agencies, payment gateways, and marketing firms, resulting in multiple points of data transfer. This increases the risk of data leakage and unauthorized access.

Additionally, there is limited awareness among consumers regarding their data privacy rights. Many customers are unaware of their rights to access, correct, or delete their personal data, which reduces accountability on the part of organizations.

Cybersecurity Challenges

The hospitality sector faces a wide range of cybersecurity challenges due to its digital infrastructure and operational complexity. One of the most critical challenges is the risk of data breaches, where unauthorized individuals gain access to sensitive customer information. Such breaches can lead to financial losses, reputational damage, and legal consequences.

Ransomware attacks are another major concern, as they can disrupt hotel operations by locking critical systems and demanding payment for restoration. Given the 24/7 nature of hospitality services, such disruptions can have severe impacts.

Phishing and social engineering attacks exploit human vulnerabilities rather than technical weaknesses. Employees who are not adequately trained in cybersecurity practices may inadvertently disclose sensitive information or grant access to malicious actors.

Legacy systems and outdated software also pose significant risks. Many hospitality businesses, especially small and medium enterprises, continue to use old systems that lack modern security features.

The increasing use of IoT devices in hotels introduces additional vulnerabilities. Devices such as smart locks, surveillance cameras, and connected appliances can be exploited if not properly secured, potentially compromising both data and physical safety.

Legal and Regulatory Framework

India's legal framework for data privacy and cybersecurity is primarily governed by the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000.

The DPDP Act establishes a comprehensive framework for the processing of personal data. It emphasizes principles such as consent, purpose limitation, data minimization, and accountability. The Act grants individuals (data principals) rights to access, correct, and erase their personal data, while imposing obligations on organizations (data fiduciaries) to ensure data protection.

The DPDP Rules, 2025 further operationalize the Act by specifying procedures for compliance, including data breach reporting and grievance redressal mechanisms.

The Information Technology Act, 2000 complements the DPDP Act by addressing cybercrime and providing legal recognition to electronic transactions. CERT-In guidelines also play a crucial role in incident reporting and cybersecurity preparedness.

Together, these regulations create a robust legal environment that requires hospitality organizations to adopt stringent data protection measures.

Impact of DPDP Act on Hospitality Sector

The implementation of the DPDP Act has significant implications for the hospitality sector. One of the most notable impacts is the need for contractual changes. Hotels must now clearly define data responsibilities in agreements with vendors and third-party service providers.

Compliance with the Act also entails increased costs, as organizations need to invest in cybersecurity infrastructure, legal expertise, and employee training. However, these investments are essential for ensuring data protection and avoiding penalties.

The Act enhances accountability by clearly defining the roles and responsibilities of data fiduciaries. Organizations are required to implement appropriate security measures and report data breaches promptly.

At the same time, the Act presents an opportunity for hospitality businesses to build customer trust. By demonstrating a commitment to data privacy, organizations can differentiate themselves in a competitive market.

Findings and Discussion

The analysis reveals that the Indian hospitality sector is at a critical juncture in terms of data privacy and cybersecurity. While digital technologies have improved efficiency and customer experience, they have also introduced significant risks.

There is a noticeable gap between regulatory requirements and industry practices. Many organizations are still in the early stages of implementing data protection measures and lack the necessary expertise and resources.

The DPDP Act has acted as a catalyst for change, encouraging organizations to adopt more structured and proactive approaches to data protection. However, challenges such as low awareness, legacy systems, and complex data ecosystems continue to hinder progress.

The findings suggest that a multi-dimensional approach involving technology, policy, and human factors is essential for addressing these challenges.

Recommendations

To enhance data privacy and cybersecurity in the hospitality sector, several strategic measures are recommended.

Organizations should invest in advanced cybersecurity technologies such as encryption, firewalls, and intrusion detection systems. Regular security audits and vulnerability assessments should be conducted to identify and mitigate risks.

Data minimization practices should be adopted to limit the collection of unnecessary information. Clear and transparent privacy policies should be communicated to customers.

Employee training programs are essential for building awareness and preventing human errors. Staff should be educated about phishing attacks, secure data handling, and incident reporting procedures.

Vendor risk management should be strengthened through strict contractual agreements and regular monitoring. Organizations should also adopt a "privacy by design" approach, integrating data protection into the development of systems and processes.

Conclusion

Data privacy and cybersecurity have emerged as critical concerns in the Indian hospitality sector due to rapid digitalization and increasing cyber threats. The introduction of the DPDP Act, 2023 marks a significant step toward establishing a robust data protection framework in India.

While the sector faces numerous challenges, including compliance gaps and technological limitations, it also has the opportunity to leverage data protection as a competitive advantage. By adopting a proactive and comprehensive approach, hospitality organizations can safeguard customer data, ensure regulatory compliance, and build long-term trust.

Ultimately, the future of the hospitality industry will depend on its ability to balance innovation with security, ensuring that technological advancements do not come at the cost of privacy and trust.

References

Government of India. (2023). Digital Personal Data Protection Act.

- Government of India. (2000). Information Technology Act.
- PwC India. (2024). Data Privacy and Consumer Awareness Report.
- EY India. (2025). Cybersecurity and DPDP Compliance Report.
- CERT-In Guidelines (Latest Edition).
- Mercan, S. et al. (2020). IoT Security in Hospitality Industry.
- Various journal articles on cybersecurity and hospitality management.